

Proposta di Modello Nazionale e Linee Guida

Versione 1.0

Sommario

Premessa	2
Definizioni	3
Modello Nazionale: Struttura e coordinamento.....	5
Linee guida per università ed enti di ricerca.....	7
Consapevolezza e comunicazione	7
Compiti dei responsabili di attività	8
Protezione dei dati e cybersecurity	8
Beni e tecnologie a rischio dual use.....	9
Collaborazioni, sovvenzioni, contratti e donazioni	10
Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi.....	10
Misure di sicurezza per i viaggi all'estero	10
Visite di personale esterno alle istituzioni di ricerca	11

Il documento è elaborato e proposto dal Gruppo di lavoro sulla sicurezza della ricerca promosso dal Ministero dell'Università e della Ricerca, di cui fanno parte esperti della materia e rappresentanti della Conferenza dei Rettori Italiani (CRUI) e della Consulta dei Presidenti degli Enti Pubblici di Ricerca (COPER). Una presentazione delle esigenze e dei criteri generali è stata fatta alla comunità dei ricercatori e accademica in occasione di due workshop tecnici organizzati nel mese di ottobre e della Conferenza Nazionale pubblica del 4 dicembre a Bari.

Il documento viene sottoposto alle valutazioni dell'apposito Tavolo interministeriale.

Premessa

Le collaborazioni internazionali, europee e nazionali, circoscritte a soggetti pubblici o estese a soggetti privati, quando forniscono vantaggi reciproci a tutte le entità coinvolte, sono componenti essenziali di una ricerca scientifica e tecnologica aperta e collaborativa, guidata dai principi di libertà e autonomia.

In questo contesto, che rimane imprescindibile per un Paese come l'Italia, occorre essere consapevoli che attività di entità straniere o comunque estranee al sistema nazionale della ricerca possono comportare crescenti criticità per l'integrità e la sicurezza di tale sistema e, in certi casi, alla sicurezza nazionale¹. Per questo, il Consiglio dell'Unione Europea ha approvato una Raccomandazione nel maggio 2024 chiedendo agli Stati membri di adottare modelli di protezione del lavoro dei ricercatori e del valore della propria ricerca nazionale.

In breve tempo, la presenza di tali modelli rappresenterà un requisito necessario per garantire la prosecuzione di collaborazioni internazionali in ambito europeo ma anche nel più ampio contesto internazionale, a partire da Stati Uniti, Regno Unito e altri Paesi G7, con cui l'Italia intrattiene rapporti di altissimo livello e qualità. È quindi nell'interesse del nostro Paese dotarsi senza ritardi di un modello adeguato.

Le ragioni che portano attori potenzialmente ostili a compromettere integrità e sicurezza della ricerca di un paese possono essere, ad esempio:

- cercare opportunità per acquisire vantaggi economici e/o tecnologici;
- impiegare tecnologie illecitamente acquisite per usi connessi alla repressione interna e/o all'attuazione di violazioni dei diritti umani o del diritto internazionale;
- reclutare competenze industriali offshore per acquisire o anticipare nel tempo risultati e/o metodi preziosi, riducendo in tal modo le capacità di altri Stati, istituzioni di ricerca o imprese potenzialmente concorrenti.

L'Italia è impegnata a garantire che al sistema nazionale delle università e degli enti di ricerca siano messi a disposizione gli strumenti e le risorse necessari per aumentare la consapevolezza e proteggere le loro attività da interferenze malevole, uso improprio e trasferimento indesiderato di conoscenze. È indispensabile, d'altra parte, che le istituzioni stesse si attivino e prendano le misure necessarie a proteggere la loro ricerca, per garantire che essa non venga sottratta e/o utilizzata a fini impropri e indesiderabili.

Quando integrità e sicurezza della ricerca, dei suoi dati, dei suoi metodi e dei suoi risultati non sono garantite in maniera adeguata, si possono avere conseguenze negative, quali ad esempio: diminuzione della fiducia nei dati e nei risultati della ricerca da parte dell'opinione pubblica; perdita/sottrazione di dati sensibili e preziosi; perdita di controllo da parte del paese sulle potenziali ricadute economiche della ricerca; danno reputazionale con, ad esempio, conseguente perdita di potenziali future collaborazioni; violazione di norme europee o nazionali.

Osservato che, sulla base di dati recenti raccolti grazie ad un questionario dedicato che ha coinvolto circa l'80 per cento delle università e degli enti di ricerca italiani, i rischi per le istituzioni di ricerca del

¹ <https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en>

nostro paese sono in aumento e possono assumere forme molteplici, è necessario uno sforzo collettivo per sviluppare e adottare misure idonee a salvaguardare integrità e sicurezza della ricerca in Italia. Pertanto, il sistema della ricerca italiano, Ministeri coinvolti, condivide la responsabilità di identificare e mitigare tali criticità. Appare inoltre strategico che le organizzazioni/istituzioni che finanziano la ricerca abbiano piena conoscenza delle potenziali criticità delle attività che vengono loro proposte, al fine di avviare un dialogo con i proponenti per la mitigazione delle criticità medesime, prima della eventuale approvazione.

All'interno di un quadro saldamente ispirato ai principi fondamentali della scienza aperta e della libertà accademica, questo modello rappresenta un primo contributo a sostegno dell'integrità e sicurezza della ricerca, quale migliore garanzia del rispetto di quei principi.

Definizioni

Nei documenti a supporto del modello nazionale per la sicurezza e integrità della ricerca e dei materiali ad esso correlati, i seguenti termini sono definiti come segue:

Collaborazioni esterne e fonti di finanziamento esterne si intendono:

- collaborazioni con soggetti/istituzioni esterni all'Unione Europea o non appartenenti a istituzioni internazionali riconosciute tramite trattati²;
- collaborazioni con soggetti non appartenenti a istituzioni pubbliche;
- finanziamenti provenienti da istituzioni esterne all'Unione Europea³ o non appartenenti a istituzioni internazionali riconosciute tramite trattati⁴;
- Finanziamenti provenienti da soggetti privati.

Istituzione / Istituzione di ricerca: termine utilizzato come alternativa per indicare università ed enti di ricerca, sia collettivamente che individualmente, a seconda del contesto.

Sicurezza e integrità della ricerca: così come definito in ambito G7 Sigre,

- **Security of research** means protecting research methods, data, and results from theft, misuse, inappropriate exploitation, and other forms of misconduct.
- **Integrity of research**, which is the direct product of integrity of researchers, is about sticking to professional values, principles, and practices that keep research honest, responsible, and societally impactful.

La definizione è ampiamente in linea con quanto definito nella Raccomandazione del Consiglio dell'Unione Europea del 23 maggio 2024 in cui la "sicurezza della ricerca" è definita come "l'anticipazione e la gestione dei rischi relativi:

a) al trasferimento indesiderato di conoscenze e tecnologie critiche che possono compromettere la sicurezza dell'Unione e dei suoi Stati membri, ad esempio se deviate verso usi militari o di intelligence in paesi terzi;

b) a ingerenze malevole nella ricerca, che possono sfociare in una sua strumentalizzazione da parte di paesi terzi con lo scopo, tra l'altro, di creare disinformazione o incoraggiare l'autocensura tra studenti e ricercatori, violando la libertà accademica e l'integrità della ricerca nell'Unione;

² Ad esempio ONU, CERN, OMS.

³ Ad esempio grant di ricerca, anche a carattere competitivo, banditi da soggetti pubblici extra-EU.

⁴ Ad esempio ONU, CERN, OMS.

c) a violazioni dell'etica o dell'integrità, in cui le conoscenze e le tecnologie sono utilizzate per reprimere, violare o minare i valori e i diritti fondamentali dell'Unione, quali definiti nei trattati.”

BOZZA

Modello Nazionale: Struttura e coordinamento

Al fine di fornire adeguato supporto alle istituzioni impegnate sui temi della sicurezza e integrità della ricerca, si attiva, a cura del Ministero dell'Università e della Ricerca, d'intesa con gli altri Ministeri interessati **e con la collaborazione supervisione della Presidenza del Consiglio**, una struttura a due livelli che contempla:

- a) un livello nazionale, provvisoriamente denominato "centro nazionale per la sicurezza e integrità della ricerca", come suggerito nella Raccomandazione del Consiglio del 23 maggio 2024⁵, che coinvolga governo (a diversi livelli), enti di ricerca e università attraverso i rispettivi organi di coordinamento;
- b) un livello locale, basato su referenti per la sicurezza e l'integrità della ricerca negli enti di ricerca e negli atenei che agiscono da elementi di collegamento tra il centro nazionale ed i singoli ricercatori, gruppi di ricerca, dipartimenti, ecc. Nelle more della individuazione dei referenti, è essenziale cominciare a sviluppare, in tutte le istituzioni di ricerca, competenze specifiche sui temi legati all'integrità ed alla sicurezza della ricerca, con la previsione di un adeguato supporto alle strutture esistenti (uffici ricerca, trasferimento tecnologico, internazionalizzazione, affari legali).

Al livello nazionale sono affidati compiti quali:

- i) realizzare e/o aggiornare linee guida e procedure per identificare interferenze indebite, **proteggere chi invia segnalazioni (whistleblower)**, **suggerire definire** livelli minimi di "due diligence" per accordi e/o collaborazioni, identificare e **proporre verificare** l'applicazione di misure a garanzia della sicurezza dei dati, dell'etica e della integrità della ricerca, tutelando altresì l'apertura internazionale ed intersettoriale attraverso gli approcci della scienza e dell'innovazione aperte, nel rispetto fondamentale della libertà della ricerca;
- ii) **fornire, su richiesta**, adeguato e tempestivo supporto alle istituzioni nella classificazione dei livelli/profili di criticità associate alla realizzazione di attività di ricerca (in particolare di quelle che prevedono collaborazioni internazionali o comunque esterne all'istituzione⁶) e nell'adozione di idonee e proporzionate misure di mitigazione;
- iii) promuovere, sviluppare e assistere, **su richiesta**, le competenze locali (referenti per la sicurezza e l'integrità della ricerca) nel monitoraggio di potenziali criticità, anche mediante la realizzazione di un supporto standard per la valutazione dei rischi che, adottato dagli organismi finanziatori della ricerca, renda omogenee e trasparenti le procedure di trasmissione e le informazioni pertinenti alla sicurezza ed integrità della ricerca associate alle domande di finanziamento;
- iv) creare occasioni di confronto e dialogo aperto con tutti gli attori del sistema della ricerca, per la condivisione di informazioni su criticità attuali ed emergenti, incluse buone pratiche e studi di caso, al fine di migliorare continuamente il livello del supporto alle misure introdotte per garantire la sicurezza e l'integrità della ricerca;
- v) realizzare e promuovere corsi di formazione sul tema delle interferenze esterne indebite, da mettere a disposizione - anche online - della comunità dei ricercatori, della governance e del personale di supporto alla ricerca;
- vi) mettere a punto un modello efficace ed efficiente per consentire un'agevole interazione con i referenti per la sicurezza e l'integrità della ricerca, da una parte, e con gli organi governativi competenti dall'altra, per segnalazioni e/o necessità di chiarimenti relativi a progetti,

⁵ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024H03510&qid=1719705121719>

⁶ Si vedano le definizioni alla pagina precedente.

collaborazioni e/o finanziamenti, anche attraverso la realizzazione di un sistema di autovalutazione preliminare che consenta di modulare il processo in funzione dei livelli/profili di rischio identificati.

Al livello locale è attribuito il compito di:

- i) informare e formare ricercatori, studenti e personale tecnico e amministrativo sulle tematiche della sicurezza ed integrità della ricerca;
- ii) sviluppare un protocollo per i visitatori, al fine di ridurre eventuali criticità durante le visite;
- iii) fornire indicazioni pertinenti ed accurate nel caso di viaggi di lavoro, in particolare verso aree (di transito o di destinazione) con profili di rischio medio-alto;
- iv) assicurare la raccolta e l'aggiornamento dei dati relativi a collaborazioni esterne in corso;
- v) contribuire alla valutazione di attività che prevedono collaborazioni o finanziamenti esterni e - ove ritenuto necessario – chiedere supporto al livello nazionale;
- vi) contribuire alla definizione di misure di mitigazione proporzionate per attività con profilo di rischio meritevole di attenzione;
- vii) fornire supporto alla definizione delle procedure da seguire in caso di problemi relativi alla sicurezza informatica che interferiscono con la sicurezza e l'integrità della ricerca, in collaborazione con i servizi informatici delle istituzioni e con le autorità nazionali competenti.

Consapevolezza e comunicazione

Distribuzione di comunicazioni a livello di istituzione - Distribuire comunicazioni tempestive ed efficaci al personale ricercatore, al personale tecnico e amministrativo, nonché ai collaboratori e agli studenti, per aumentare la consapevolezza e fornire informazioni sull'influenza indebita da parte di eventuali attori potenzialmente malevoli (governi ed entità straniere e/o estranee al sistema nazionale della ricerca). Queste comunicazioni includono (ad esempio) informazioni su: azioni che i ricercatori possono intraprendere per mitigare possibili criticità; sui referenti a cui rivolgersi per assistenza; requisiti e responsabilità per la segnalazione, la divulgazione, il controllo del trasferimento di conoscenze e tecnologie e altri controlli di sicurezza previsti dalle norme nazionali o europee.

Pubblicazione di newsletter e presentazioni sulla sicurezza - Pubblicare e distribuire periodicamente newsletter sulla sicurezza riguardanti temi quali, a titolo di esempio, i rischi provenienti dall'estero e la preparazione per viaggi internazionali; organizzare seminari e presentazioni su integrità e sicurezza della ricerca rivolti ad audience specifiche (tesisti, dottorandi, ricercatori senior, project leaders, leadership accademiche ecc.).

Creazione di pagine web ad hoc nei siti istituzionali - Creare e mettere in evidenza nei siti web istituzionali pagine con link e informazioni su una vasta gamma di argomenti, quali: impegni di ricerca internazionali e collaborazione globale, influenze e interferenze indebite (per esempio, ma non solo, di governi stranieri) e mitigazione dei relativi rischi. Il sito web deve servire anche come 'sportello unico' per accedere alle politiche e pratiche dell'istituzione in tema di integrità e sicurezza della ricerca, alle relative comunicazioni e informazioni, alle linee guida, nonché ai requisiti definiti dalle istanze nazionali (Governo, Ministeri, ecc.). Sarà presente il link al sito appositamente realizzato dal Ministero: <https://www.sicurezza Ricerca.mur.gov.it>.

Promozione del confronto nella comunità - Promuovere discussioni durante le riunioni degli organi di governo dell'istituzione e della comunità di ricerca (ricercatori e personale tecnico e amministrativo coinvolto). Favorire incontri regolari a livello delle strutture interne (dipartimenti, istituti, divisioni ecc.) sui vari aspetti della integrità e sicurezza della ricerca.

Formazione - Organizzare moduli formativi su tematiche quali: integrità e sicurezza della ricerca, linee di condotta per viaggi e soggiorni all'estero, linee di condotta in presenza di visitatori nelle strutture, protezione dei dati e cyber-security, attività soggette a controllo delle esportazioni, protezione della proprietà intellettuale.

A tal proposito, il Ministero dell'Università e della Ricerca ha realizzato una serie di moduli formativi - che saranno aggiornati all'occorrenza - disponibili sul sito web dedicato <https://www.sicurezza Ricerca.mur.gov.it>, nella sezione "Formazione".

Compiti dei responsabili di attività

I responsabili di progetti di ricerca, programmi di collaborazione scientifica e didattica, attività di ricerca o innovazione commissionata, o conto terzi o spin off sono tenuti, prima dell'avvio della loro attività, a prendere conoscenza del modulo formativo "Integrità e Sicurezza", reperibile nella sezione "Formazione" del sito <https://www.sicurezzaaricerca.mur.gov.it>. A seguire, condurranno un'autovalutazione preliminare delle eventuali criticità associate alla attività da intraprendere accedendo all'area dedicata del sito [sicurezzaaricerca.mur.gov.it](https://www.sicurezzaaricerca.mur.gov.it) per compilare la scheda di autovalutazione.

Se l'attività non implica il **coinvolgimento di partner e/o finanziamenti esterni** (si veda la definizione a pagina 3), sarà sufficiente dichiararlo. Diversamente, il responsabile effettuerà un'analisi secondo tre possibili categorie di criticità, cioè quelle connesse a) all'ambito scientifico o tecnologico nel quale si colloca l'attività, b) alle persone e alle istituzioni con cui si collabora, c) alle entità che finanziano le attività. Per ciascuna categoria, saranno presi in considerazione sia i rischi teoricamente possibili, sia quelli concretamente associati all'attività. Una volta riempiti i campi della scheda, verrà automaticamente calcolato, per ciascuna categoria, un **valore dei rischi** associati all'attività. In base ad essi, il responsabile otterrà un report con misure da adottare per mitigare le criticità indicate, ed eventualmente il suggerimento di rivolgersi al referente per la sicurezza e l'integrità della ricerca dell'istituzione di appartenenza per ottenere ulteriori indicazioni al fine di condurre l'attività. Il referente, qualora ne ravvisi la necessità, informando i responsabili dell'attività ed autorizzato dal responsabile legale dell'istituzione o suo delegato, potrà rivolgersi al centro nazionale per la sicurezza ed integrità della ricerca per opportuni ragguagli.

Il responsabile dell'attività potrà valutare di rivolgersi al proprio referente per la sicurezza e l'integrità della ricerca anche prima o durante la compilazione della scheda, qualora necessiti di un confronto preventivo per una migliore valutazione delle criticità associate alla propria attività. Sarà inoltre suo compito aggiornare la scheda di autovalutazione dell'attività in ogniqualvolta ricorrano modifiche riguardo collaborazioni e finanziamenti o ogni altra evoluzione delle attività che possa variare il livello di rischio.

Protezione dei dati e cybersecurity

Consapevolezza di rischi informatici nel contesto delle attività di ricerca scientifica – Informare e formare ricercatori, studenti e personale amministrativo e tecnico sulla sicurezza informatica di base, sulle misure di protezione dei dati e sulle implicazioni della cybersecurity nella protezione delle attività di ricerca. Anche su questo aspetto, sono previsti moduli formativi nel sito www.sicurezzaaricerca.mur.gov.it alla sezione "Formazione".

Analisi e misure di gestione del rischio – Condurre una analisi per la valutazione del rischio cyber associato alle attività di ricerca scientifica, coinvolgendo le parti interessate: personale ricercatore e personale tecnico amministrativo dedicato (servizi IT). Sviluppare un framework di gestione del rischio cyber delle attività di ricerca che includa l'identificazione degli asset informativi critici, la protezione dei dati, il controllo degli accessi, la gestione dell'identità, la sicurezza delle reti e dei sistemi informativi e le procedure di risposta agli incidenti. Le istituzioni collaborano con l'Agenzia

per la Cybersecurity Nazionale⁷ (ACN) - con particolare riferimento alla conformità alla direttiva NIS-2, con il Garante per la Protezione dei Dati Personali⁸ (GPDP), con l’Agenzia per l’Italia Digitale⁹ (AGID), e le altre autorità competenti.

Sicurezza informatica e sicurezza della ricerca – Adottare misure per la sicurezza informatica delle attività di ricerca e la prevenzione delle violazioni interne proporzionate al livello di rischio, alla criticità della specifica attività e alle altre informazioni di contesto.

Aggiornamento continuo – Monitorare i cambiamenti normativi e adottare pratiche di miglioramento continuo, con particolare riferimento alle norme comunitarie e nazionali, in collaborazione con le autorità competenti e il centro nazionale per la sicurezza e l’integrità della ricerca.

Beni e tecnologie a rischio dual use

I beni e le tecnologie che hanno la caratteristica di essere stati progettati per applicazioni civili ma che potrebbero eventualmente essere malversati in applicazioni belliche/nucleari in grado di sfuggire al monitoraggio dedicato a questo tipo di applicazioni sono regolamentati a livello comunitario e nazionale.

L’attività di ricerca, costantemente innovativa, è particolarmente esposta a processi di trafugamento e/o esportazione non autorizzata di beni e tecnologie. Inoltre, vi è anche la possibilità che entità ed organismi, estranee agli obiettivi pacifici della ricerca, siano interessate a raccogliere informazioni, conoscenze e materiale scientifico eventualmente utilizzabili in applicazioni non monitorate o vincolate da stati di embargo internazionale.

Al fine di mitigare criticità provenienti da queste esposizioni l’Italia, come gli altri Stati europei, ha dedicato un’apposita struttura, l’Unità UAMA¹⁰ del Ministero per gli Affari Esteri e la Cooperazione Internazionale, per supportare l’attività di imprese e istituzioni di ricerca nella gestione di questi rischi, come da Regolamento EU 821/2021¹¹ e successivi aggiornamenti ed adottando un Piano di Controllo della Tecnologia come previsto dalla Raccomandazione EU 1700/2021¹² emessa a specifico supporto di accademie ed enti di ricerca.

Per ulteriori informazioni relative alla gestione delle attività di cui al presente paragrafo si rimanda ai siti web delle autorità competenti e alla sezione “Risorse” del sito web <https://www.sicurezzaericerca.mur.gov.it>.

⁷ <https://www.acn.gov.it/portale/home>

⁸ <https://www.garanteprivacy.it/>

⁹ <https://www.agid.gov.it/it>

¹⁰ <https://www.esteri.it/it/ministero/struttura/uama/>

¹¹ <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021R0821>

¹² <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32021H1700>

Collaborazioni, sovvenzioni, contratti e donazioni

Utilizzare la scheda di autovalutazione e misure per la mitigazione dei rischi forniti dal centro nazionale per la sicurezza e l'integrità della ricerca, a complemento del necessario buon senso, per l'analisi di progetti, collaborazioni, contratti, accordi, sovvenzioni e donazioni, ogniqualvolta siano coinvolte entità esterne (si veda definizione iniziale). L'analisi dovrà includere il controllo delle eventuali esportazioni di tecnologie, la valutazione dei termini e condizioni delle sovvenzioni e la potenziale generazione e trasmissione all'esterno di dati o informazioni sensibili. Per le situazioni che richiedono uno screening aggiuntivo, i ricercatori si rivolgeranno al referente per la sicurezza e l'integrità della ricerca dell'istituzione, il quale, a sua volta, valuterà se opportuno interfacciarsi con il centro nazionale per la sicurezza e l'integrità della ricerca.

Revisione, aggiornamento e applicazione delle politiche di conflitto di interessi

Un Conflitto di Interesse (COI) indica qualsiasi circostanza in cui gli interessi personali, professionali, finanziari o di altro tipo di un individuo (inclusi i membri immediati della sua famiglia) possono potenzialmente o effettivamente divergere, o possono essere ragionevolmente percepiti come potenzialmente o effettivamente divergenti, dai suoi obblighi professionali verso l'istituzione di appartenenza e dagli interessi dell'istituzione stessa. Un COI può esistere ogniqualvolta un osservatore indipendente possa ragionevolmente mettere in dubbio che le azioni o decisioni professionali dell'individuo, inclusa la condotta etica e obiettiva di studi, ricerche o attività cliniche, siano influenzate da considerazioni di guadagno personale, finanziario o di altro tipo. Le situazioni di COI si possono instaurare qualora il singolo ricercatore abbia interessi scientifici, finanziari o didattici con soggetti esterni all'istituzione di appartenenza. In questo ambito rientrano affiliazioni, relazioni e interessi che possono entrare in conflitto con le responsabilità del ricercatore verso la propria istituzione. A titolo di esempio, si menziona la partecipazione a programmi di reclutamento, l'attribuzione di posizioni accademiche, le collaborazioni (anche a titolo non retribuito), il ruolo di "principal investigator" in progetti in cui non è coinvolta l'istituzione di appartenenza.

Si raccomanda alle istituzioni che già hanno nei rispettivi ordinamenti dei codici di condotta relativi a COI di valutare la coerenza con le presenti linee guida, mentre alle istituzioni che non le avessero ancora, si raccomanda di adottarle. A supporto dei ricercatori le cui istituzioni di appartenenza non abbiano ancora emanato dei codici di condotta, si suggerisce di visionare la sezione relativa al COI nell'area "Risorse" del sito <https://www.sicurezza Ricerca.mur.gov.it>.

Misure di sicurezza per i viaggi all'estero

Sviluppare o aggiornare vademecum per viaggi internazionali e prevedere un registro per tenerne traccia. Fornire briefing sulla sicurezza personalizzati, se necessario, per destinazioni o scopi del viaggio con margini di criticità non trascurabili.

Le istituzioni faranno riferimento al modulo formativo "Regole di base per Viaggi e Soggiorni all'Estero", che verrà reso disponibile nella sezione "Formazione" del sito governativo <https://www.sicurezza Ricerca.mur.gov.it> e si accerteranno che i ricercatori ne abbiano preso conoscenza prima d'intraprendere il viaggio.

Visite di personale esterno alle istituzioni di ricerca

Sviluppare o aggiornare regolamenti per disciplinare visite di personale esterno nelle istituzioni di ricerca. Prevedere registri per l'accesso al fine di tenere traccia di elementi quali: visitatore/i, scopo della visita, personale interno incontrato, durata. Anche in questo caso, per le strategie da adottare le istituzioni faranno riferimento al modulo formativo "Protocollo per la gestione delle visite", che verrà reso disponibile nella sezione "Formazione" del sito governativo <https://www.sicurezza.mur.gov.it>. Le istituzioni si accerteranno che i responsabili dell'accoglienza abbiano preso conoscenza della risorsa formativa prima della visita.

BOLZA